CLAIMS

1. A terminal device for transferring a right to use content to a portable medium while protecting a copyright of the content, comprising:

a storage unit storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content;

a decryption unit operable to decrypt the first encrypted content using the device key, to generate the content;

a conversion unit operable to perform an irreversible conversion on the generated content, to generate converted content;

an encryption unit operable to encrypt the converted content using the medium key, to generate second encrypted content;

a write unit operable to move the medium key and the second encrypted content to the portable medium, and read the device key from the storage unit and write the read device key to the portable medium; and

a key deletion unit operable to delete the device key from the storage unit.

2. The terminal device of Claim 1,

wherein the key deletion unit deletes the device key from the storage unit after the write unit writes the device key to the portable medium, and

the write unit moves the medium key and the second

encrypted content to the portable medium after the key deletion unit deletes the device key from the storage unit.

3. The terminal device of Claim 2,

wherein the storage unit further stores key information for encrypting the device key,

the encryption unit further encrypts the device key using the key information; and

the write unit writes the encrypted device key to the portable medium, as the device key.

4. The terminal device of Claim 3 after the write unit writes the encrypted device key to the portable medium, the key deletion unit deletes the device key from the storage unit, and the write unit moves the medium key and the second encrypted content to the portable medium, further comprising:

a read unit operable to read the encrypted device key from the portable medium,

wherein the decryption unit further decrypts the read encrypted device key using the key information to generate the device key, and stores the generated device key to the storage unit.

5. The terminal device of Claim 1, further comprising:

an embedment unit operable to embed the device key in the converted content, to generate key-embedded content,

wherein the encryption unit encrypts the key-embedded content using the medium key, to generate the second encrypted

content,

the key deletion unit deletes the device key from the storage unit after the embedment unit embeds the device key in the converted content, and

the write unit moves the medium key and the second encrypted content to the portable medium after the key deletion unit deletes the device key from the storage unit.

6. The terminal device of Claim 5 after the key deletion unit deletes the device key from the storage unit and the write unit moves the medium key and the second encrypted content to the portable medium, further comprising:

an extraction unit operable to extract the device key from the key-embedded content, and store the extracted device key to the storage unit,

wherein a read unit reads the second encrypted content and the medium key from the portable medium, and

the decryption unit further decrypts the read second encrypted content using the read medium key to generate the key-embedded content, and outputs the generated key-embedded content to the extraction unit.

7. The terminal device of Claim 1 after the write unit writes the device key to the portable medium, the key deletion unit deletes the device key from the storage unit, and the write unit moves the medium key and the second encrypted content to the portable medium, further comprising:

a read unit operable to read the device key from the

portable medium,

wherein the read unit stores the read device key to the storage unit.

8. The terminal device of Claim 7, further comprising:

a reproduction unit operable to reproduce the content,

wherein the decryption unit further reads the first encrypted content and the device key from the storage unit, decrypts the read first encrypted content using the read device key to generate the content, and outputs the generated content to the reproduction unit.

9. A content protection system for transferring a right to use content from a terminal device to a portable medium while protecting a copyright of the content,

the terminal device comprising:

a first storage unit storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content;

a decryption unit operable to decrypt the first encrypted content using the device key, to generate the content;

a conversion unit operable to perform an irreversible conversion on the generated content, to generate converted content;

an encryption unit operable to encrypt the converted content using the medium key, to generate second encrypted content;

a write unit operable to move the medium key and the

second encrypted content to the portable medium, and read the device key from the first storage unit and write the read device key to the portable medium; and

a key deletion unit operable to delete the device key from the first storage unit, and

the portable medium comprising:

a second storage unit operable to store the device key, the medium key, and the second encrypted content received from the terminal device,

wherein the key deletion unit deletes the device key from the first storage unit after the write unit writes the device key to the second storage unit, and

the write unit moves the medium key and the second encrypted content to the portable medium after the key deletion unit deletes the device key from the first storage unit.

10. The content protection system of Claim 9 after the write unit writes the device key to the portable medium, the key deletion unit deletes the device key from the first storage unit, and the write unit moves the medium key and the second encrypted content to the portable medium,

wherein the terminal device further comprises:

a read unit operable to read the device key form the second storage unit,

the read unit stores the read device key to the first storage unit,

the portable medium further comprises:

a deletion unit operable to delete at least one of the

second encrypted content and the medium key from the second storage unit, and

the read unit reads the device key from the second storage unit after the deletion unit deletes the at least one of the second encrypted content and the medium key from the second storage unit.

11. The content protection system of Claim 9,

wherein the first storage unit further stores key information for encrypting the device key,

the encryption unit further encrypts the device key using the key information,

the write unit writes the encrypted device key to the second storage unit as the device key, and after writing the encrypted device key, moves the medium key and the second encrypted content to the second storage unit, and

the second storage unit stores the encrypted device key as the device key.

12. The content protection system of Claim 11 after the write unit writes the encrypted device key to the second storage unit, the key deletion unit deletes the device key from the first storage unit, and the write unit moves the medium key and the second encrypted content to the second storage unit,

wherein the terminal device further comprises:

a read unit operable to read the encrypted device key from the second storage unit,

wherein the decryption unit further decrypts the read

encrypted device key using the key information to generate the device key, and stores the generated device key to the first storage unit,

the portable medium further comprises:

a deletion unit operable to delete at least one of the second encrypted content and the medium key from the second storage unit, and

the read unit reads the encrypted device key from the second storage unit after the deletion unit deletes the at least one of the second encrypted content and the medium key from the second storage unit.

13. The content protection system of Claim 9,

wherein the terminal device further comprises:

an embedment unit operable to embed the device key in the converted content, to generate key-embedded content,

the encryption unit encrypts the key-embedded content using the medium key, to generate the second encrypted content,

the key deletion unit deletes the device key from the first storage unit after the embedment unit embeds the device key in the converted content, and

the write unit writes the medium key and the second encrypted content to the second storage unit after the key deletion unit deletes the device key from the first storage unit.

14. The content protection system of Claim 13 after the key deletion unit deletes the device key from the first storage

unit and the write unit moves the medium key and the second encrypted content to the second storage unit,

wherein the terminal device further comprises:

an extraction unit operable to extract the device key from the key-embedded content, and store the extracted device key to the first storage unit,

a read unit reads the second encrypted content and the medium key from the second storage unit,

the decryption unit further decrypts the read second encrypted content using the read medium key to generate the key-embedded content, and outputs the generated key-embedded content to the extraction unit, and

the portable medium deletes the second encrypted content and the medium key from the second storage unit after the terminal device reads the second encrypted content and the medium key from the second storage unit.

15. The content protection system of Claim 9, further including a mobile information terminal,

wherein the mobile information terminal reads, from the portable medium in which the device key, the medium key, and the second encrypted content are stored in the second storage unit, the second encrypted content and the medium key, decrypts the read second encrypted content using the read medium key to generate the converted content, and reproduces the converted content.

16. The content protection system of Claim 9, further including

another terminal device connected with the terminal device,

wherein the another terminal device comprises:

a read unit operable to read, from the portable medium in which the device key, the medium key, and the second encrypted content are stored in the second storage unit, the device key, the medium key, and the second encrypted content;

a deletion unit operable to delete at least one of the medium key and the second encrypted content read by the read unit; and

an acquisition unit operable to acquire the first encrypted content from the terminal device, after the deletion unit deletes the at least one of the medium key and the second encrypted content,

the portable medium moves the device key, the medium key, and the second encrypted content to the another terminal device, and

the terminal device further comprises:

a transmission unit operable to transmit the first encrypted content to the another terminal device; and

a content deletion unit operable to delete the first encrypted content from the first storage unit.

17. A portable medium for receiving a right to use content from a terminal device while protecting a copyright of the content, a recording device including: a storage unit storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content; a decryption unit operable to decrypt the first

encrypted content using the device key, to generate the content; a conversion unit operable to perform an irreversible conversion on the generated content, to generate converted content; an encryption unit operable to encrypt the converted content using the medium key, to generate second encrypted content; a write unit operable to move the medium key and the second encrypted content to the portable medium, and read the device key from the first storage unit and write the read device key to the portable medium; and a key deletion unit operable to delete the device key from the first storage unit,

the portable medium comprising:

a storage unit operable to store the device key, the medium key, and the second encrypted content.

18. A content movement method used in a terminal device for transferring a right to use content to a portable medium while protecting a copyright of the content, the terminal device storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content, the content movement method comprising:

a decryption step of decrypting the first encrypted content using the device key, to generate the content;

a conversion step of performing an irreversible conversion on the generated content, to generate converted content;

an encryption step of encrypting the converted content using the medium key, to generate second encrypted content;

a write step of moving the medium key and the second

encrypted content to the portable medium, and reading the device key from the storage unit and writing the read device key to the portable medium; and

a key deletion step of deleting the device key from the terminal device.

19. The content movement method of Claim 18,

wherein the key deletion step deletes the device key from the terminal device after the write step writes the device key to the portable medium, and

the write step moves the medium key and the second encrypted content to the portable medium after the key deletion step deletes the device key from the terminal device.

20. A content movement program used in a terminal device for transferring a right to use content to a portable medium while protecting a copyright of the content, the terminal device storing first encrypted content, a device key, and a medium key, the first encrypted content being generated by encrypting the content, the content movement program comprising:

a decryption step of decrypting the first encrypted content using the device key, to generate the content;

a conversion step of performing an irreversible conversion on the generated content, to generate converted content;

an encryption step of encrypting the converted content using the medium key, to generate second encrypted content;

a write step of moving the medium key and the second

encrypted content to the portable medium, and reading the device key from the storage unit and writing the read device key to the portable medium; and

a key deletion step of deleting the device key from the terminal device.

21. The content movement program of Claim 20,

wherein the key deletion step deletes the device key from the terminal device after the write step writes the device key to the portable medium, and

the write step moves the medium key and the second encrypted content to the portable medium after the key deletion step deletes the device key from the terminal device.